NEW YORKSTATE MODEL DATA PRIVACY AGREEMENT
FOR EDUCATIONAL AGENCIES

St. Lawrence-Lewis BOCES and Component Districts

and

Teacher's Discovery (Flangoo)

This Data Privacy Agreement ("DPA") is by and between St. Lawrence-Lewis BOCES and including its 18 component school districts each with their individual Bill of Rights for Data Security and Privacy: Brasher Falls, Canton Central, Clifton-Fine Central, Colton-Pierrepont Central, Edwards-Knox Central, Gouverneur Central, Hammond Central, Harrisville Central, Hermon-DeKalb Central, Heuvelton Central, Lisbon Central, Massena Central, Morristown Central, Madrid-Waddington Central, Norwood-Norfolk Central, Ogdensburg City, Parishville-Hopkinton Central and Potsdam Central, here by deemed as ("EA"), an Educational Agency, and Teacher's Discovery, collectively, the "Parties".

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.

2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.

3. **Disclose**: To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.

4. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.

5. **Educational Agency**: As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.

6. **Eligible Student:** A student who is eighteen years of age or older.

7. **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.

8. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Frameworkfor Improving Critical Infrastructure Cybersecurity Version 1.1.

9. **Parent:**Aparent, legal guardian or person in parental relation to the Student.

10. **Personally Identifiable Information (PII):**Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and Teacher or Principal APPR Data, as defined below.

11. **Release:** Shall have the same meaning as Disclose.

12. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law §3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law §4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.

13. **Student:** Any person attending or seeking to enroll in an Educational Agency.

14. **Student Data:**Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.

15. **Subcontractor:**Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.

16. **Teacher or Principal APPR Data**: Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. **Compliance with Law.**
   In order for Contractor to provide certain services ("Services")to the EA pursuant to a contract dated 11/1/2024 ("Service Agreement"); Contractor may receive PIIregulated by several New Yorkand federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA")

at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New YorkEducation Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federaland local laws, rules and regulations.

2. **Authorized Use.**

   Contractor has no property or licensing rights or claims of ownership toPII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. **Data Security and Privacy Plan**.

   Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies withNew YorkState, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. **EA's Data Security and Privacy Policy**

   State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

5. **Right of Review and Audit.**

   Upon request by the EA, Contractor shall provide the EA with copies of its policies andrelated procedures that pertain to the protection of PII. It may be made availablein a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may berequired to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the

EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. **Contractor's Employees and Subcontractors**.

   (a)   Contractor shall only disclose PII to Contractor's employees and subcontractorswho need to know the PII in order toprovide the Services and the disclosure of PII shall be limited tothe extent necessary to provide such Services.Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.

   (b)   Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.

   (c)   Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materiallycomply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breachreporting requirements set forth herein.

   (d)   Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.

   (e)   Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. **Training**.

   Contactor shall ensure that all its employeesand Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. **Termination**

   The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retainaccess to PII.

9. Data Return and Destruction of Data.

(a)　　　Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII,in a format agreed to by the Parties to the EA.

(b)　　　If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed.Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.

(c)　　　Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.

(d)　　　To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII oruseor disclose PII for a Commercial or Marketing Purpose.

11. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New Yorklaw and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New Yorklaws and regulations.

12. Breach.

(a)   Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven(7) business days after discovery of the Breach.Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), orby registered or certified, and must to the extent available, include a description of the Breachwhich includes the date of the incident and the date of discovery;the types of PII affected and the number of records affected;a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EAshall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b)   Notifications required under this paragraph must be provided to the EA at the following address:

Darin Saiff, Assistant Superintendent of Instruction
40 West Main St
Canton, NY 13617
dpo@sllboces.org

13. Cooperation with Investigations.

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractorif such Breach is attributable to Contractor or its Subcontractors.

14. Notification to Individuals.

Where a Breachof PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

15. **Termination**.

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. **Parent and Eligible Student Access**.

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. **Bill of Rights for Data Privacy and Security**.

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively,and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. **Priority of Agreements and Precedence.**

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditionsof this DPA shall govern and prevail,shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. **Execution.**

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.
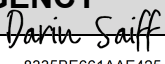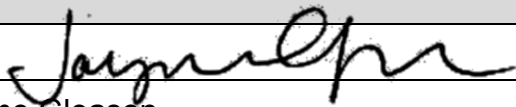
EDUCATIONAL AGENCY	CONTRACTOR
BY: *Darin Saiff* 8335BE661AAE425...	BY: *(signature)*
Darin Saiff	Jayme Gleason
Data Privacy Officer	Bid/Contract Coordinator
Date: 11/5/2024 | 5:48 AM PST	Date: 11/1/2024

EXHIBIT A- Education Law §2-d Bill of Rights for Data Privacy and Security for
St. Lawrence-Lewis BOCES Bill of Rights for Data Security and Privacy

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketingpurpose.PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. Therighttoinspectandreviewthecompletecontentsofthestudent'seducationrecordstoredormaintainedby aneducationalagency. This right may not apply to Parents of an Eligible Student.

3. State andfederal laws such asEducation Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protecttheconfidentialityofastudent's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available atwww.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA, Darin Saiff, dpo@sllboces.org, 315-386-4504 (ii) Complaints may also be submitted to the NYSEducation Department atwww.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email toprivacy@nysed.gov; or by telephone at518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PIIoccurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protectPII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and securityrequirements.

Education Law §2-d Bill of Rights for Data Privacy and Security for
Brasher Falls Central School/ St. Lawrence Central School District

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketingpurpose.PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. Therighttoinspectandreviewthecompletecontentsofthestudent'seducationrecordstoredormaintainedby aneducationalagency. This right may not apply to Parents of an Eligible Student.

3. State andfederal laws such asEducation Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protecttheconfidentialityofastudent's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available atwww.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA, Kevin Welsh, Director of Data and Technology, P.O Box 307, Brasher Falls, NY 13613 orkwelsh@bfcsd.org(ii) Complaints may also be submitted to the NYS Education Department atwww.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email toprivacy@nysed.gov; or by telephone at518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PIIoccurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protectPII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and securityrequirements.

Education Law §2-d Bill of Rights for Data Privacy and Security for
Canton Central School District

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketingpurpose.PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. Therighttoinspectandreviewthecompletecontentsofthestudent'seducationrecordstoredormaintainedby aneducationalagency. This right may not apply to Parents of an Eligible Student.

3. State andfederal laws such asEducation Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protecttheconfidentialityofastudent's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available atwww.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA, Tim Archetko tarchetko@ccsdk12.org315-386-8561(ii) Complaints may also be submitted to the NYS Education Department atwww.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email toprivacy@nysed.gov; or by telephone at518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PIIoccurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protectPII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and securityrequirements.

Education Law §2-d Bill of Rights for Data Privacy and Security for
Clifton Fine Central School District

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketingpurpose.PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. Therighttoinspectandreviewthecompletecontentsofthestudent'seducationrecordstoredormaintainedby aneducationalagency. This right may not apply to Parents of an Eligible Student.

3. State andfederal laws such asEducation Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protecttheconfidentialityofastudent's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available atwww.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA, Matt Southwick, msouthwick@cliftonfine.org 315-848-3333(ii) Complaints may also be submitted to the NYS Education Department atwww.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email toprivacy@nysed.gov; or by telephone at518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PIIoccurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protectPII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and securityrequirements.

Education Law §2-d Bill of Rights for Data Privacy and Security for
Colton-Pierrepont Central School District

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketingpurpose.PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. Therighttoinspectandreviewthecompletecontentsofthestudent'seducationrecordstoredormaintainedby aneducationalagency. This right may not apply to Parents of an Eligible Student.

3. State andfederal laws such asEducation Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protecttheconfidentialityofastudent's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available atwww.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA, Jim Nee, jnee@cpcs.us, 315-262-2100 (ii) Complaints may also be submitted to the NYS Education Department atwww.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email toprivacy@nysed.gov; or by telephone at518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PIIoccurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protectPII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and securityrequirements.

Education Law §2-d Bill of Rights for Data Privacy and Security for
Edwards-Knox Central School District

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketingpurpose.PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. Therighttoinspectandreviewthecompletecontentsofthestudent'seducationrecordstoredormaintainedby aneducationalagency. This right may not apply to Parents of an Eligible Student.

3. State andfederal laws such asEducation Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protecttheconfidentialityofastudent's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available atwww.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA, Erin Woods, ewoods@ekcsk12.org 315-562-8130 (ii) Complaints may also be submitted to the NYS Education Department atwww.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email toprivacy@nysed.gov; or by telephone at518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PIIoccurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protectPII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and securityrequirements.

Education Law §2-d Bill of Rights for Data Privacy and Security for
Gouverneur Central School District

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketingpurpose.PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. Therighttoinspectandreviewthecompletecontentsofthestudent'seducationrecordstoredormaintainedby aneducationalagency. This right may not apply to Parents of an Eligible Student.

3. State andfederal laws such asEducation Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protecttheconfidentialityofastudent's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available atwww.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA: Jackie Kelly,kelly.jackie@gcsk12.org315-287-4914 (ii) Complaints may also be submitted to the NYS Education Department atwww.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email toprivacy@nysed.gov; or by telephone at518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PIIoccurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protectPII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and securityrequirements.

Education Law §2-d Bill of Rights for Data Privacy and Security for
Hammond Central School District

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketingpurpose.PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. Therighttoinspectandreviewthecompletecontentsofthestudent'seducationrecordstoredormaintainedby aneducationalagency. This right may not apply to Parents of an Eligible Student.

3. State andfederal laws such asEducation Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protecttheconfidentialityofastudent's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available atwww.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA: Lauren Morely, lmorely@hammondk12.org 315-324-5931(ii) Complaints may also be submitted to the NYS Education Department atwww.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email toprivacy@nysed.gov; or by telephone at518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PIIoccurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protectPII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and securityrequirements.

Education Law §2-d Bill of Rights for Data Privacy and Security for
Harrisville Central School District

Parents (includes legal guardians or persons in parental relationships) and Eligible Students (student 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as defined by Education Law § 2-d and FERPA, includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including but not limited to encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at http://www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. Complaints may be submitted to NYSED at http://www.nysed.gov/data-privacysecurity/report-improper-disclosure, by mail to:
Mr. Robert Finster, Superintendent of Schools, 14371 Pirate Lane, Harrisville, NY 13648 or at rfinster@hcsk12.org. Complaints to SED should be directed to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; the e-mail address is cpo@mail.nysed.gov.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

Education Law §2-d Bill of Rights for Data Privacy and Security for

Hermon-Dekalb Central School District

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketingpurpose.PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. Therighttoinspectandreviewthecompletecontentsofthestudent'seducationrecordstoredormaintainedby aneducationalagency. This right may not apply to Parents of an Eligible Student.

3. State andfederal laws such asEducation Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protecttheconfidentialityofastudent's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available atwww.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA: Mark White, mwhite@hdcsk12.org 315-347-3442 (ii) Complaints may also be submitted to the NYS Education Department atwww.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email toprivacy@nysed.gov; or by telephone at518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PIIoccurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protectPII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and securityrequirements.

Education Law §2-d Bill of Rights for Data Privacy and Security for
Heuvelton Central School District

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketingpurpose.PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. Therighttoinspectandreviewthecompletecontentsofthestudent'seducationrecordstoredormaintainedby aneducationalagency. This right may not apply to Parents of an Eligible Student.

3. State andfederal laws such asEducation Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protecttheconfidentialityofastudent's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available atwww.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA: Data Protection Officer, District Superintendent, 315-344-2414 x28891(ii) Complaints may also be submitted to the NYS Education Department atwww.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email toprivacy@nysed.gov; or by telephone at518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PIIoccurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protectPII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and securityrequirements.

Education Law §2-d Bill of Rights for Data Privacy and Security for
Lisbon Central School District

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketingpurpose.PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. Therighttoinspectandreviewthecompletecontentsofthestudent'seducationrecordstoredormaintainedby aneducationalagency. This right may not apply to Parents of an Eligible Student.

3. State andfederal laws such asEducation Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protecttheconfidentialityofastudent's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available atwww.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA: Data Protection Officer, farrandp@lisbonk12.ny.us, 315-393-4951 (ii) Complaints may also be submitted to the NYS Education Department atwww.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email toprivacy@nysed.gov; or by telephone at518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PIIoccurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protectPII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and securityrequirements.

Education Law §2-d Bill of Rights for Data Privacy and Security for
Madrid-Waddington Central School District

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketingpurpose.PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. Therighttoinspectandreviewthecompletecontentsofthestudent'seducationrecordstoredormaintainedby aneducationalagency. This right may not apply to Parents of an Eligible Student.

3. State andfederal laws such asEducation Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protecttheconfidentialityofastudent's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available atwww.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA: Data Protection Officer, 2582 St. Hwy 345, Madrid, NY 13660 or eburke@mwcsk12.org, 315-322-5746(ii) Complaints may also be submitted to the NYS Education Department atwww.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email toprivacy@nysed.gov; or by telephone at518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PIIoccurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protectPII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and securityrequirements.

Education Law §2-d Bill of Rights for Data Privacy and Security for
Massena Central School District

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1.   A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketingpurpose.PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2.   Therighttoinspectandreviewthecompletecontentsofthestudent'seducationrecordstoredormaintainedby aneducationalagency. This right may not apply to Parents of an Eligible Student.

3.   State andfederal laws such asEducation Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protecttheconfidentialityofastudent's identifiable information.

4.   Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5.   A complete list of all student data elements collected by NYSED is available atwww.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY12234.

6.   The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA: Data Protection Officer, rburke@mcs.k12.ny.us, 315-764-3700(ii) Complaints may also be submitted to the NYS Education Department atwww.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email toprivacy@nysed.gov; or by telephone at518-474-0937.

7.   To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PIIoccurs.

8.   Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protectPII.

9.   Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and securityrequirements.

Education Law §2-d Bill of Rights for Data Privacy and Security for
Morristown Central School District

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketingpurpose.PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. Therighttoinspectandreviewthecompletecontentsofthestudent'seducationrecordstoredormaintainedby aneducationalagency. This right may not apply to Parents of an Eligible Student.

3. State andfederal laws such asEducation Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protecttheconfidentialityofastudent's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available atwww.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA: Morristown Central School, 408 Gouverneur St. PO Box 217, Morristown, NY 13664, dpo@mcsk12.org or by telephone at 315-375-8814 (ii) Complaints may also be submitted to the NYS Education Department atwww.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email toprivacy@nysed.gov; or by telephone at518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PIIoccurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protectPII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and securityrequirements.

Education Law §2-d Bill of Rights for Data Privacy and Security for
Norwood-Norfolk Central School District

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketingpurpose.PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. Therighttoinspectandreviewthecompletecontentsofthestudent'seducationrecordstoredormaintainedby aneducationalagency. This right may not apply to Parents of an Eligible Student.

3. State andfederal laws such asEducation Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protecttheconfidentialityofastudent's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available atwww.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA: Superintendent, James Cruikshank, Norwood-Norfolk Central School, 7852 State Highway 56, Norwood, NY 13668,by email to jcruikshank@nncsk12.org or by telephone at 315-353-6631. (ii) Complaints may also be submitted to the NYS Education Department atwww.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email toprivacy@nysed.gov; or by telephone at518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PIIoccurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protectPII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and securityrequirements.

Education Law §2-d Bill of Rights for Data Privacy and Security for
Ogdensburg Central School District

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketingpurpose.PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. Therighttoinspectandreviewthecompletecontentsofthestudent'seducationrecordstoredormaintainedby aneducationalagency. This right may not apply to Parents of an Eligible Student.

3. State andfederal laws such asEducation Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protecttheconfidentialityofastudent's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available atwww.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA: Data Protection Officer, 1100 State Street, Ogdensburg NY 13669, by email to kkendall@ogdensburgk12.org or by telephone at 315-393-0900. (ii) Complaints may also be submitted to the NYS Education Department atwww.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email toprivacy@nysed.gov; or by telephone at518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PIIoccurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protectPII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and securityrequirements.

Education Law §2-d Bill of Rights for Data Privacy and Security for
Parishville-Hopkinton Central School District

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketingpurpose.PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. Therighttoinspectandreviewthecompletecontentsofthestudent'seducationrecordstoredormaintainedby aneducationalagency. This right may not apply to Parents of an Eligible Student.

3. State andfederal laws such asEducation Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protecttheconfidentialityofastudent's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available atwww.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EAData Protection Officer, 12 County Route 47, Parishville, NY 13672, by email to scoffin@phcsd.org or by telephone at 315-265-4642 (ii) Complaints may also be submitted to the NYS Education Department atwww.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email toprivacy@nysed.gov; or by telephone at518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PIIoccurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protectPII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and securityrequirements.

Education Law §2-d Bill of Rights for Data Privacy and Security for
Potsdam Central School District

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketingpurpose.PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. Therighttoinspectandreviewthecompletecontentsofthestudent'seducationrecordstoredormaintainedby aneducationalagency. This right may not apply to Parents of an Eligible Student.

3. State andfederal laws such asEducation Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protecttheconfidentialityofastudent's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available atwww.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA:Data Protection Officer, 29 Leroy Street, Potsdam, NY 13676, by email to dpo@potsdam.ny.k12.us, or by telephone at 315-265-2000 (ii) Complaints may also be submitted to the NYS Education Department atwww.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email toprivacy@nysed.gov; or by telephone at518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PIIoccurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protectPII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and securityrequirements.
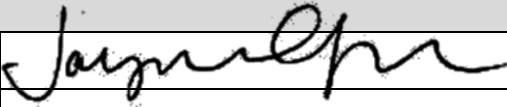
CONTRACTOR's Signature of acceptance of each Bill of Rights as above	
[Signature]	*Jayme Gleason (signature)*
[Printed Name]	Jayme Gleason
[Title]	Bid/Contract Coordinator
Date:	11/1/2024

EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -

SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law §2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	Teacher's Discovery (Flangoo)
Description of thepurpose(s) for which Contractor will receive/access PII	Flangoo Digital Reader Subscription is a web based World Language reader library for your teaching needs.
Type of PII thatContractor will receive/access	Check all that apply: ☑Student PII ☑APPR Data
Contract Term (Annual fiscal cycle)	Contract Start Date _____7/1/2024_____ Contract End Date _____6/30/2027_____
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requiresthe subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) ☐Contractor will not utilize subcontractors. ☑ Contractor will utilize subcontractors.

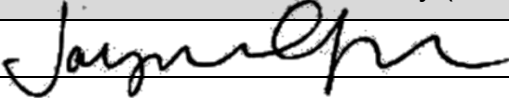|	
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties**.** • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractoragrees to facilitate such corrections within 21 days of receiving the EA's written request.
Secure Storage and Data Security	Please describe where PII will be storedand the protections taken to ensure PII will be protected: (check all that apply) ☑ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: please visit https://flangoo.com/general/privacypolicy
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR American Eagle Company Inc., DBA Teacher's Discovery (Flangoo)	
[Signature]	
[Printed Name]	Jayme Gleason
[Title]	Bid/Contract Coordinator
Date:	11/1/2024

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	SSL, Multiple Firewalls, Data Encryption
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Limited information collected, Data Encryption
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Online Courses, Confidentiality Agreements
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	Confidentiality Agreements
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	Breach plan outlined on the website https://flangoo.com/general/privacypolicy
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Can be transferred upon request
7	Describe your secure destruction practices and how certification will be provided to the EA.	Student data will be deleted after 6 months of subscription inactivity
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Compliant with current policies